IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JANIELLE DAWSON, individually and on behalf of all others similarly situated, Plaintiff, v. NATIONAL UNIVERSITY, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Janielle Dawson ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action suit brought on behalf of all persons all persons in the United States who purchased a degree program and/or course offered by National University ("Defendant") during the Class Period, as that term is defined below.

2. Plaintiff brings this action in response to Defendant's practice of integrating, installing and embedding third-party tracking technology, including the tracking technology of Meta Platforms, Inc., formerly known as Facebook, Inc. ("Facebook"), into nu.edu and its affiliated web propoerties (the "Website") and thereby: (a) knowingly disclosing to third parties its users' personally identifiable information ("PII"), including their video-watching behavior; and (b) allowing the third parties to intercept and obtain users' federally-protected and confidential education records.

3. Defendant's conduct, as alleged herein, violates the Video Privacy Protection Act, 18 U.S.C. § 2710, *et seq.* ("VPPA"); the Electronic Communications and Privacy Act, 18 U.S.C. § 2510, *et seq.* ("ECPA"); the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.* ("CIPA"); and the Illinois Eavesdropping Act, 720 Ill. Comp. Stat. 5/14-1, *et seq*.

PARTIES

Plaintiff

4. Plaintiff Janielle Dawson is, and has been at all relevant times, a resident of Cook County, Illinois and has an intent to remain there, and is therefore a domiciliary of Illinois. Plaintiff created a Facebook account in approximately 2008. Beginning in or around September 2023, Plaintiff enrolled in a degree program at National University to obtain a Bachelor of Arts Degree in Psychology. Plaintiff enrolled at National University via Defendant's Website. In connection with her degree program, Plaintiff has regularly enrolled in numerous online class courses offered by Defendant. As recently as early 2024, Plaintiff enrolled in an online course offered by Defendant.

5. In connection with her degree program at National University, Plaintiff took online class courses that included, but were not limited to: (a) Introduction to Psychology; (b) Principles of Sociology; (c) Survey of Bioscience; (d) Introduction to Art History; and (e) Introduction to Interpersonal Communications.

6. In connection with her coursework at National University, Plaintiff used the Website to, *inter alia*, view prerecorded videos, obtain and turn in assignments, communicate with faculty, take tests, view her transcript and grades and pay for courses and tuition.

7. Plaintiff's class courses routinely included prerecorded videos, which Plaintiff watched in connection with her coursework. Plaintiff's video-watching behavior was to watch prerecorded National University videos in connection with completing her coursework.

8. Every time Plaintiff used the Website, including when she enrolled in her degree program and specific courses, the Website was running tracking technology offered by Facebook and known as the Facebook Tracking Pixel, among other third-party tracking technologies – including tracking technologies offered by Google LLC ("Google"); ByteDance, also known as TikTok ("TikTok"); Hotjar, Ltd. ("Hotjar"); Microsoft Corporation ("Microsoft"); and Amazon.com, Inc. ("Amazon") (collectively, with Facebook, the "Third-Party Tracking Companies") – which Defendant used to: (a) disclose Plaintiff's video-watching behavior, among other personally identifiable information, to Facebook and the other Third-Party Tracking Companies; and (b) allow the Third-Party Tracking Companies to intercept and obtain Plaintiff's federally-protected and confidential education records.

9. Defendant's Website utilized full-string, descriptive URLs that contained detailed information regarding the webpage being viewed by a user. For example, the webpage associated with information about a Bachelor of Arts Degree in Psychology is https://www.nu.edu/degrees/social-sciences/programs/bachelor-arts-psychology/.

10. Plaintiff did not discover or otherwise become aware of Defendant's unlawful conduct, as alleged herein, until approximately February 2025.

Defendant

11. Defendant National University is a private nonprofit education system comprised of university and education-related affiliates. Defendant is headquartered in San Diego, California.

Defendant owns and operates the Website, which is used throughout Illinois, California and the United States.

12. Defendant is a post-secondary education institution that is required to comply with the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g ("FERPA"), and its implementing regulations.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under laws of the United States.

14. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

15. This Court has personal jurisdiction over Defendant because Defendant disclosed Plaintiff's PII in this District. Further, Defendant purposefully availed itself of the privilege of conducting business in Illinois and/or purposefully directed its activities at the state by, *inter alia*, advertising in Illinois and recruiting students in Illinois. Moreover, the injuries of Plaintiff and Class members relate to Defendant's forum-related activities. Finally, the exercise of jurisdiction comports with traditional notions of fair play and substantial justice.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claim occurred in this District.

FACTUAL BACKGROUND

I. The VPPA

17. The genesis of the VPPA was President Ronald Reagan's nomination of Judge Robert Bork to the United States Supreme Court. During the confirmation process, a movie rental store disclosed Bork's rental history to the Washington City Paper, which then published it. Congress responded by passing the VPPA, with an eye toward the digital future. As Senator

Patrick Leahy, who introduced the Act, explained:

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. In an area of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong.

S. Rep. 100-599, at 5-6 (internal ellipses and brackets omitted).

18. A violation of the VPPA occurs when "[a] video tape service provider . . . knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

19. The VPPA defines "consumer" as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1).

20. The VPPA defines personally identifiable information as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider" (hereinafter "VPPA PII"), 18 U.S.C. § 2710(a)(3). Information constitutes VPPA PII if it readily permits an ordinary person to identify a specific individual's video-watching behavior.

21. The VPPA defines "video tape service provider" as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

II. The FERPA

22. FERPA and its implementing regulations govern the release of, and access to, "education records." *See* 20 U.S.C. § 1232(g); 34 C.F.R. Part 99.

23. Under the FERPA, "education records" are "those records, files, documents, and other materials which – (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." 20 U.S.C. § 1232g(a)(4)(A).

24. Under the regulations implementing the FERPA, "personally identifiable information" includes, but is not limited to: (a) the name of the student's parent or other family members; (b) a personal identifier, such as the student's social security number or biometric record; (c) other indirect identifiers such as the maiden name of a student's mother; (d) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in a school community who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and (e) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the educational record relates (hereinafter "FERPA PII"). 34 C.F.R. 99.3.

25. Under the FERPA, an educational institution or agency may not disclose education records or personally identifiable information contained therein without signed and dated written consent, subject to exceptions not applicable here. *See* 34 C.F.R. 99.30, 99.31.

III. Facebook and the Facebook Tracking Pixel

26. Facebook is the largest social networking site on the planet, touting 2.9 billion monthly active users. Facebook describes itself as a "real identity platform,"[1] meaning users are allowed only one account and must share "the name they go by in everyday life."[2] To that end,

[1] *Sam Schechner and Jeff Horwitz, How Many Users Does Facebook Have? The Company Struggles to Figure It Out,* WALL. ST. J. (Oct. 21, 2021).
[2] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

when creating an account, users must provide their first and last name, along with their birthday and gender.

27. Facebook generates revenue by selling advertising space on its website.

28. Facebook sells advertising space by highlighting its ability to target users.[3] Facebook can target users so effectively because it surveils user activity both on and off its site. This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[4] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[5]

29. Advertisers can also build "Custom Audiences."[6] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website." Advertisers can use a Custom Audience to target existing customers directly, or they can use it to build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[7] Unlike Core Audiences, Custom Audiences require an advertiser to supply the underlying data to Facebook. They can do so through two mechanisms: by manually uploading contact information for

[3] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.
[4] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[5] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.
[6] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.
[7] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

customers, or by utilizing Facebook's "Business Tools," which collect and transmit the data automatically. One such Business Tool is the Facebook Tracking Pixel.

30. As the name implies, the Facebook Tracking Pixel "tracks the people and type of actions they take."[8] When a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Tracking Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites—Defendant's own code and Facebook's embedded code.

31. An example illustrates the point. Take an individual who navigates to one of Defendant's websites and clicks on a tab for allergy information. When that tab is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Because Defendant utilizes the Facebook Tracking Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly and concurrently duplicate the communication with the Website, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

32. Once this record is received, Facebook processes it, analyzes it, and assimilates it into datasets like the Core Audiences and Custom Audiences.

[8] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

33. Further, once Facebook intercepts users' communications on the Website, Facebook has the ability to use the intercepted information for its own purposes beyond recording the information for Defendant. Facebook benefits from the information it collects from its clients' websites, such as Defendant's students who visit the Website, because Facebook uses this information to improve its advertising network, including its machine-learning algorithms and its ability to target users with ads.[9]

34. Advertisers control what actions—or, as Facebook calls it, "events"—the Facebook Tracking Pixel will collect, including the website's metadata, along with what pages a visitor views and what buttons a visitor clicks. Advertisers can also configure the Facebook Tracking Pixel to track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases. An advertiser can also create their own tracking parameters by building a "custom event."

35. Advertisers control how the Facebook Tracking Pixel identifies visitors. The Facebook Tracking Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific Data."[10] HTTP Headers collect "IP addresses, information about the web browser, page location, document, referrer and persons using the website."[11] Pixel-specific Data includes "the Pixel ID and cookie."[12]

IV. Google's Platform and Its Business Tools

36. Google offers a range of advertising software, one of which is called Google Analytics.

[9] FACEBOOK, PRIVACY POLICY, https://www.facebook.com/privacy/policy/.
[10] FACEBOOK, FACEBOOK PIXEL, https://developers.facebook.com/docs/meta-pixel/.
[11] *Id.*
[12] *Id*.

37. "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights" for businesses.[13] This is made possible by Google Analytics, a piece of code installed on a website or app that collects information on how website and app users interact with a business's website, including "how many users bought an item . . . by tracking whether they made it to the purchase-confirmation page."[14]

38. Google advertises that this service can "[m]onitor activity on your site as it happens."[15]

39. Google's business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners' websites with Google Analytics.

40. Thus, through websites and apps that employ Google's services, Google directly receives the electronic communications of website visitors entered into websites via website and app features like search bars.

41. That information is then analyzed by Google before it is provided to any entity that was a party to the conversation (like Defendant). In order to conduct this analysis, Google, on information and belief, views the information.

42. Once Google intercepts website or app communications, it has the capability to use such information for its own purposes. "Google uses the information shared by sites and apps to deliver [] services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on [] partners' sites and apps."[16]

---

[13] GOOGLE, HOW GOOGLE ANALYTICS WORKS, https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=2827624563183915220-NC.
[14] *Id.*
[15] GOOGLE, THE FINER POINTS, https://marketingplatform.google.com/about/analytics/features/.
[16] GOOGLE, GOOGLE PRIVACY AND TERMS, https://policies.google.com/technologies/partner-sites.

43. Google's range of software services is based on Google's ability to collect and analyze information about consumers' web behavior and deliver targeted advertising to select consumers based on their web habits. This involves collecting visitor information from thousands of websites and then analyzing that information in order to group web users so they can be targeted for products or services based on their interests.

44. In order to engage in analyzing the collected data to deliver targeted advertising, Google, on information and belief, regularly viewed and used the personally identifiable information and education records of University of Phoenix students collected by the Google Analytics code. As such, on information and belief, Google regularly viewed and used Plaintiff's and Class members' PII, including video-watching behavior, and education records and the information contained therein intercepted via Google Analytics.

45. Information from websites, like Defendant's Website, is central to Google's ability to successfully market its advertising capabilities to future clients.

46. In sum, Google has the capability to use website and app communications to: (a) improve its own products and services; (b) develop new Google for Business and Google Analytics products and services; and (c) analyze website visitors' communications to assist with and data analytics and targeted advertising.

47. Defendant shares information with Google that amounts to PII via its collection of device identifiers and IP addresses. Google uses IP addresses and unique device identifiers to track internet users. Therefore, Defendant is disclosing PII to Google as described in the section below.

48. Yet another type of PII obtained from website users by Google, and subsequently viewed by Google, is what data companies refer to as a "browser-fingerprint." A browser-

fingerprint is information collected about a computing device that can be used to identify the specific device.

49. These browser-fingerprints provide a wide variety of data and can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked. As Google has explained, "[w]ith fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[17] The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[18] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.[19]

50. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[20]

51. Browser-fingerprints are personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

52. On information and belief, Defendant uses and causes the disclosure of data sufficient for third parties, like Google, to create a browser-fingerprint identifier with each re-directed communication described herein, including student communications concerning video-watching behavior and education records.

---

[17] GOOGLE, BUILDING A MORE PRIVATE WEB, https://www.blog.google/products/chrome/building-a-more-private-web/.
[18] Chris Hauk, *What is Browser Fingerprinting? How it Works and How to Stop it*, https://pixelprivacy.com/resources/browser-fingerprinting/.
[19] *Supra* note 37.
[20] Yinzhi Cao, Song Li & Erik Wijmans, *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/.

V. TikTok and the TikTok Tracking Pixel

53. TikTok offers a software-as-a-service ("SaaS") called "TikTok Tracking Pixel," which "helps businesses track the performance of their ads" by sending information from the business's website to TikTok, which then uses that information to optimize ad campaigns on TikTok and across the internet.[21]

54. The TikTok Tracking Pixel can be "plugged in" to any website, as the pixel is a piece of code that can be added to any website to capture "events" (*i.e.*, any activity by a user that happens on a website).

55. The TikTok Tracking Pixel is part of a package of prebuilt software tools under the "TikTok for Business" product line that allow for the delivery of personalized ads. By employing TikTok to collect user information through the TikTok Tracking Pixel, websites that procure TikTok's services can use the information to deliver more effective targeted advertisements, increasing revenue for the websites.

56. In short, when users interact with a webpage in which the TikTok Tracking Pixel is integrated, embedded and/or installed, the TikTok Tracking Pixel collects the "Metadata and button clicks" (*i.e.*, information about what the user clicked on—such as the specific URL address visited by the user— or text entered into the webpage), a timestamp for the event, and the visitor's IP address.[22] That information is sent automatically to TikTok.

57. The "TikTok for Business" business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners' websites with the TikTok Tracking Pixel.

[21] "TikTok Pixel 101: What It Is & How to Use It," https://popupsmart.com/blog/tiktok-pixel
[22] "About TikTok Pixel," https://ads.tiktok.com/help/article/tiktok-pixel?redirected=2

58. Thus, through websites that employ TikTok's services, TikTok directly receives the electronic communications of website visitors in real time.

59. On Defendant's Website, TikTok collected the URL value of the page visited, an identification code TikTok uses to track the user, and the visitor's browser type and operating system.

60. Once TikTok intercepts website communications, it has the capability to use such information for its own purposes. TikTok's Commercial Terms of Service grant TikTok "a non-exclusive, royalty-free, worldwide, transferable, sublicensable license to access, use, host, cache, store, display, publish, distribute, modify and adapt [information collected from partner websites] in order to develop, research, provide, promote, and improve TikTok's products and services."[23]

61. In practice, this means the information collected is used to: (a) analyze trends in consumer behavior based on data collected from websites across the internet that TikTok can then use when providing targeted advertising to other companies; (b) create consumer profiles of specific users, allowing TikTok to sell future customers targeted advertising to consumers with specific profile characteristics; and (c) develop new TikTok Business products and services, or improve pre-existing TikTok Business products and services.

62. One of TikTok's partners was Defendant. The TikTok Tracking Pixel was employed on the Website in the manner described throughout this Complaint.

VI. Hotjar and Session Replay Technology

63. At relevant times, Defendant integrated and embedded into the Website session replay technology offered by Hotjar.

[23] "TikTok For Business Commercial Terms of Service," https://ads.tiktok.com/i18n/official/policy/commercial-terms-of-service

64. Session replay technology, as noted in a 2017 piece by Princeton University researchers, is "unlike typical [internet] analytics services [like cookies] that provide aggregate statistics[.] [Rather,] these scripts are intended for the recording and playback of individual browsing sessions, as if someone is looking over your shoulder." [24] That is, session replay works by "embedded snippets of code . . . [that] watch and record a visitor's every move on a website, in real time."[25]

65. Hotjar explains in a page titled "How do Recordings Work: Advanced Explanation[,]" that "[r]ecordings are created . . . [by] captur[ing] the data from your site during a user's session."[26] "When a user opens a webpage where Hotjar is installed, a WebSocket connection is established. This connection is a real-time communication channel between the user's browser and Hotjar's servers."[27] "After the WebSocket is opened, Hotjar captures the initial HTML content and DOM tree from the recorded user's session . . . using the [Mozilla] Mutation Observer API[.]"[28] Per Mozilla, "Document Object Model (DOM) is the data representation of the objects that comprise the structure and content of a document on the web."[29]

66. The end result is that a Hotjar session replay wiretap provides real-time recordings of users' interactions on the Website, while those interactions are being transmitted

[24] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts* (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[25] Tomas Foltyn, *What's the Deal with Session-Replay Scripts?*, Welivesecurity (Apr. 20, 2018), https://www.welivesecurity.com/2018/04/20/whats-deal-session-replay-scripts/.
[26] Hotjar, *How Do Recordings Work: Advanced Explanation*, https://help.hotjar.com/hc/en-us/articles/21825186925207-How-do-Recordings-Work-Advanced-Explanation.
[27] *Id.*
[28] *Id.*
[29] Mozilla Corporation, *Introduction to the DOM*, https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model/Introduction.

over the internet. That is, Hotjar uses session replay to surreptitiously intercept and/or record in real-time, the keystrokes, mouseclicks and movement, scrolling, data entry, and/or other electronic communications of Website users.

67. Hotjar states: "Recordings . . . [v]isually captur[e] interactions such as clicks, mouse movements, scroll behavior, and keystrokes[,] offer[ing] profound insights into user engagement, pain points, and preferences."[30] Hotjar makes clear, "[b]y piecing together each action within a session, Hotjar generates comprehensive recordings that reflects user behavior on the website, which can then be analyzed further."[31]

68. Session replay technology is not widely known by the public. Most website owners do not disclose the use of session replay technology on their websites out of fear of unnerving website visitors and suppressing website traffic. Any disclosures in privacy policies are futile, because by the time anyone will have seen such a disclosure, the session replay technology will have already been deployed.

69. Further, as a 2017 study by Princeton University researchers recognized, "the extent of data collected by these services ***far exceeds expectations***[]; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous."[32]

70. Session replay technology is not only highly intrusive, it is dangerous. The 2017 study by Princeton University researchers found that session replay technologies were collecting

[30] Hotjar, *How Do Recordings Work: Advanced Explanation*, https://help.hotjar.com/hc/en-us/articles/21825186925207-How-do-Recordings-Work-Advanced-Explanation.
[31] *Id.*
[32] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts* (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

sensitive user information such as passwords and credit card numbers. The research notes that this was not simply the result of a bug, but rather, insecure practices.[33] Thus, session replay technologies such as those operated by Hotjar can leave users vulnerable to data leaks and the harms resulting therefrom.

71. By integrating and embedding Hotjar into the Website, Defendant allowed Hotjar to surreptitiously intercept and record interactions between Website users, on the one hand, and Defendant, on the other.

VII. Microsoft and Amazon

72. Defendant also integrated, embedded and installed into the Website software code created by Microsoft called bat.bing. Bat.bing collects Microsoft's Machine Unique Identifier (MUID cookie) from users. This cookie is a unique user identifier and remains active for one year. It is used for advertising, site analytics, and other operational purposes.

73. Defendant also integrated, embedded and installed into the Website software code created by Amazon that functioned in a manner similar to the above-described software code of Facebook, Google, LinkedIn, TikTok and Microsoft.

VIII. National University's Use of Third-Party Tracking Technologies

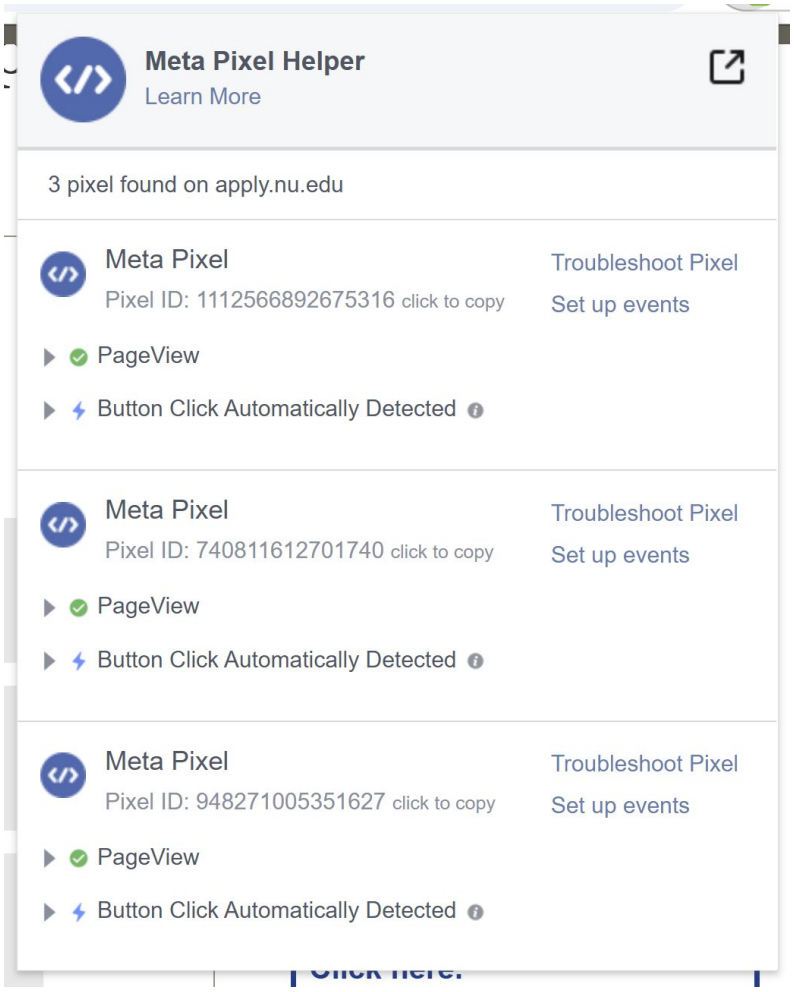
74. National University is one of the largest online universities in the United States. It sells degree programs and single courses, both of which are taught using prerecorded videos.

75. When purchasing a degree program, a single course, or when enrolling in a course, each step of the purchase/enrollment process is monitored by the Facebook Tracking Pixel and the tracking technologies offered by the Third-Party Tracking Companies, among others. Upon

[33] *Id.*

information and belief, the Facebook Tracking Pixel also monitors every video course that students view and sends data about those videos to Facebook without the users' knowledge or consent.

76. For instance, when applying to National University, three separate Facebook Tracking Pixels are running on the online application:



77. On each of these pages of the Website, the Facebook Tracking Pixel is configured to send Facebook PageView and Button Click data, which includes information about the goods and services the student seeks to obtain.

In addition, the Website contains the code for at least eight different Facebook cookies:

Name	Value	Domain
ar_debug	1	.facebook.com
fr	1Kq9fq7JHUW9YkQvO.AW...	.facebook.com
c_user	679395441	.facebook.com
ps_n	1	.facebook.com
xs	27%3AasgrOb2ovNSlPQ%3...	.facebook.com
sb	_MvhZhEX7ZeI9FAjN0dTN-n5	.facebook.com
datr	9cvhZr5vG9HVMmQsnsSu...	.facebook.com
ps_l	1	.facebook.com

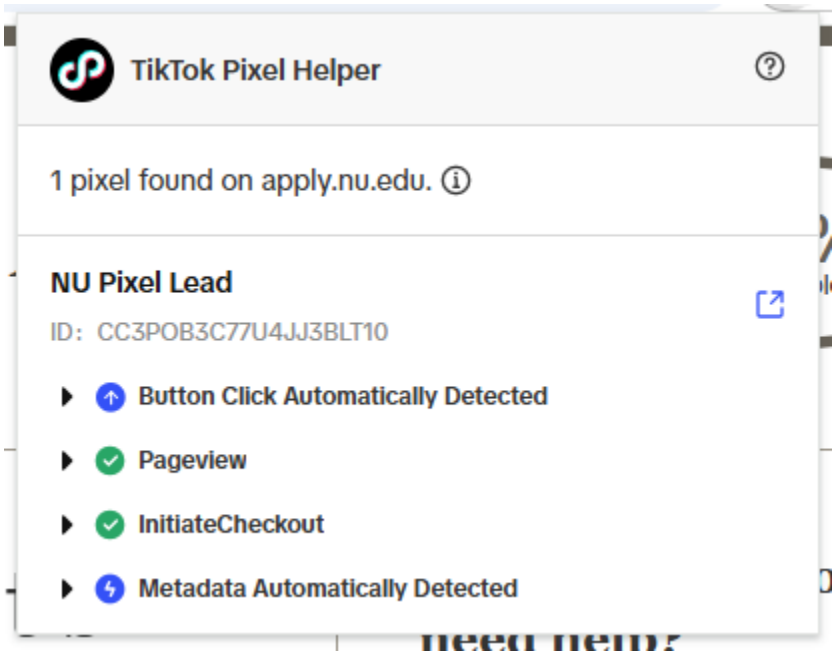
78. When someone who is logged into Facebook enrolls in a degree program or course on the Website, the Facebook Tracking Pixel transmits PII from these Facebook cookies to Facebook along with the person's PageView and Button Click data. For instance, the c_user cookie contains a visitor's Facebook ID.

79. A Facebook ID is PII. Anyone can identify a Facebook profile—and all personal information publicly listed on that profile—by appending the Facebook ID to the end of facebook.com.

80. The combination of the PageView and Button Click data and the PII from Facebook's cookies embedded on the Website permits Facebook to see who enrolled in what course or degree program offered by Defendant.

81. As alleged above, the Website also contains tracking technologies from other third parties.

82. For instance, the Website contains the TikTok Tracking Pixel:



83. The Website also contains the code for a Tik Tok cookie:

Name	Value	Domain
_ttp	2uYKpiQq25s6wvjHzh...	.tiktok.com

84. On information and belief, Defendant discloses, and otherwise allows the interception, of the PII and communications described herein in order to generate increased profits by way of, *inter alia*: (a) targeted advertisements that are based on students' video-watching behavior, education records and other PII; (b) improved course offerings; and (c) offering a more user-friendly website.

IX. Plaintiff's and Class Members' Reasonable Expectation of Privacy

85. At relevant times, Plaintiff and Class members had a reasonable expectation of privacy in their: (a) video-watching behavior; and (b) education records and the information contained therein.

86. Indeed, pursuant to FERPA, Defendant was not permitted to disclose a student's education records and the PII contained therein without signed and dated written consent, subject to exceptions not applicable here.

87. Similarly, pursuant to the VPPA, Defendant was not permitted to disclose a consumer's video-watching behavior without obtaining consent.

88. Nevertheless, as a result of Defendant procuring numerous third parties to intercept the Website communications of Plaintiff and Class members, each time Plaintiff and Class members used the Website, the third parties intercepted and obtained Plaintiff's and Class members' education records and the information contained therein without consent. Moreover, when students purchased and enrolled in classes or a degree program, Defendant disclosed their video-watching behavior without consent.

CLASS ALLEGATIONS

89. Plaintiff brings this action, pursuant to Federal Rule of Civil Procedure 23, individually and on behalf of the following class and subclass:

(a) **Class Definition:** Plaintiff seeks to represent a class of similarly situated individuals defined as all persons in the United States who purchased a degree program and/or course from Defendant during the Class Period.

(b) **Illinois Subclass Definition:** Plaintiff seeks to represent a class of similarly situated individuals defined as all Illinois residents who purchased a degree program and/or course from Defendant during the Class Period.

90. Subject to additional information obtained through further investigation and discovery, the above-described Class and Subclass may be modified or narrowed as appropriate, and additional subclasses may be defined.

91. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations – after considering any tolling, concealment and accrual issues – and ending on the date of entry of any judgment.

92. **Numerosity (Fed. R. Civ. P. 23(a)(1)):** At this time, Plaintiff does not know the exact number of members of the aforementioned Class. However, given the popularity of the Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

93. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2), 23(b)(3)):** There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

(a) whether Defendant collected Plaintiff's and the Class's PII and video purchasing activity;

(b) whether Defendant unlawfully disclosed and continues to disclose its users' PII and video purchasing activity in violation of the VPPA;

(c) whether Defendant's disclosures were committed knowingly;

(d) whether Defendant disclosed Plaintiff's and the Class's PII and video purchasing activity without consent;

(e) whether Defendant procured third parties to intercept the communications of Plaintiff and the Class;

(f) whether Facebook, Hotjar, Microsoft, Google, TikTok and Amazon were third-party eavesdroppers; and

(g) whether Plaintiff and Class members are entitled to damages under the VPPA, the Federal Wiretap Act and other relevant statute.

94. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiff's claims are typical of those of the Class because Plaintiff, like all members of the Class, used Defendant's Website to watch

prerecorded videos, and had her PII and video purchasing activity collected and disclosed by Defendant.

95. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, including litigation concerning the VPPA. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor her counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional representatives to represent the Class, additional claims as may be appropriate, or to amend the definition of the Class to address any steps that Defendant took.

96. **Superiority (Fed. R. Civ. P. 23(b)(3)):** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights

of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action.

CAUSES OF ACTION

COUNT ONE
Violation of the Video Privacy Protection Act
18 U.S.C. § 2710, *et seq.*
(On behalf of Plaintiff and the Class)

97. Plaintiff restates and realleges the allegations of paragraphs 1 through 96, above, as though fully set forth herein.

98. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

99. Defendant is a "video tape service provider" because it "engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4). As alleged herein, Defendant delivers and sells prerecorded videos to University of Phoenix students, including Plaintiff and Class members, via the Website.

100. Plaintiff and members of the Class are "consumers" because, at relevant times, they were renters, subscribers and/or purchasers of goods and services from Defendant, namely class and degree programs that included prerecorded videos as part of their content. 18 U.S.C. § 2710(a)(1).

101. Defendant disclosed to the third parties, including the Third-Party Tracking Companies, Plaintiff's and Class members' PII as defined by the VPPA. Defendant utilized the tracking technologies offered by the Third-Party Tracking Companies to compel Plaintiff's and Class members' web browsers to transfer Plaintiff's and Class members' identifying information,

like their Facebook IDs, along with Plaintiff's and Class members' event data, including information about the videos they viewed.

102. Plaintiff and the Class members enrolled in degree programs and courses via the Website, where they also viewed Defendant's prerecorded videos.

103. Defendant knowingly disclosed Plaintiff's PII, as defined by the VPPA, because it knowingly installed the tracking technologies of the Third-Party Tracking Companies on the Website.

104. Plaintiff and Class members did not provide Defendant with any form of consent, written or otherwise, to disclose their PII, as defined by the VPPA, to third parties.

105. Defendant's disclosures were not made in the "ordinary course of business" as the term is defined by the VPPA. In particular, Defendant's disclosures to the Third-Party Tracking Companies were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2).

COUNT TWO
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq.*
(On behalf of Plaintiff and the Class)

106. Plaintiff restates and realleges the allegations of paragraphs 1 through 96, above, as though fully set forth herein.

107. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

108. Under the ECPA, it is unlawful for a person to intentionally intercept, endeavor to intercept or procure any other person to intercept or endeavor to intercept any wire, oral or electronic communication. 18 U.S.C. § 2511(1)(a).

109. Under the ECPA, it is unlawful for a person to intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

110. The ECPA protects both the sending and receipt of communications.

111. Under the ECPA, a "person" includes "any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

112. Under the ECPA, in relevant part, "electronic communication" means:

> any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce or foreign commerce . . . .

18 U.S.C. § 2510(12).

113. Under the ECPA, "'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

114. Under the ECPA, in relevant part, "'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication . . . ." 18 U.S.C. § 2510(5).

115. The following constitute "devices" within the meaning of 18 U.S.C. § 2105(5):

(a) The computer codes and programs of the Third-Party Tracking Companies used to intercept, monitor, capture and record Plaintiff's and Class members' communications and data transmissions while they were accessing and navigating the Website;

(b) Plaintiff's and Class members' browsers;

(c) Plaintiff's and Class members' computing and mobile devices;

(d) The web servers of the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members';

(e) The web servers from which the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members intercepted Plaintiff's and Class members' communications while they were using a web browser to access and navigate the Website;

(f) The computer codes and programs used by the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members to effectuate their interception and recording of Plaintiff's and Class members' communications while they were using a browser to access and navigate the Website;

(g) The plan the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members carried out to effectuate their interception of Plaintiff's and Class members' communications while they were using a web browser or mobile application to access and navigate the Website; and

(h) The code of the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members embedded, integrated and installed into the Website.

116. Under the ECPA, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [the ECPA] may in a civil action recover

from the person or entity . . . which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2520(a).

117. Under the ECPA, the "court may assess as damages whichever is the greater of – (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000." 18 U.S.C. § 2520(c)(2). Additional appropriate relief includes: (a) equitable or declaratory relief; (b) punitive damages; and (c) a reasonable attorney's fee and other litigation costs reasonably incurred. 18 U.S.C. § 2520(b).

118. Defendant was, and continue to be, a "person" under the ECPA.

119. In violation of the ECPA, 18 U.S.C. § 2511(1)(a), Defendant intentionally procured various third parties, including the Third-Party Tracking Companies, to intercept and endeavor to intercept the electronic communications of Plaintiff and Class members, namely the transmissions of the confidential and sensitive information of Plaintiff and Class members via the Website, including education records and the information contained therein, as well as their video-watching behavior. At relevant times, Defendant knew that by integrating, installing and embedding the third-party tracking technology described herein, the Third-Party Tracking Companies would intercept the electronic communications of users of the Website.

120. In violation of the ECPA, 18 U.S.C. § 2511(1)(d), Defendant used, or endeavored to use, the contents of the electronic communications of Plaintiff and Class members to generate profits and increase revenues by, *inter alia*, attempting to increase its enrollment through targeted advertising and improve its course offerings based on an analysis of the intercepted communications, knowing and having reason to know that the information was obtained through

the unlawful interception of the electronic communications of Plaintiff and Class members, in violation of the ECPA, as alleged herein.

121. Defendant knew and had reason to know that it procured the third parties to intercept the electronic communications at issue and used the fruits thereof in violation of the ECPA, as Defendant did not obtain Plaintiff's and Class members' consent to intercept the electronic communications and, as alleged below, did so for criminal and tortious purposes.

122. At the time of the above-described electronic communications, Plaintiff and Class members exhibited an expectation that the communications were not subject to interception under circumstances justifying such an expectation, as alleged herein.

123. Plaintiff and Class members did not consent to the interception and disclosure of their sensitive and confidential electronic communications via the Website.

124. At the time Defendant intentionally procured third parties – including the Third-Party Tracking Companies – to intercept and endeavor to intercept the electronic communications of Plaintiff and Class members, Defendant was not acting under color of law.

125. Defendant procured third parties – including the Third-Party Tracking Companies – to intercept and endeavor to intercept the electronic communications of Plaintiff and Class members for the purpose of: (a) violating the VPPA; (b) violating the FERPA; (c) violating the CIPA; and (d) violating the Illinois Eavesdropping Act, 720 Ill. Comp. Stat. 5/14-1, *et seq.*

126. Plaintiff and Class members seek all relief to which they are entitled under the ECPA, including statutory damages, punitive damages, equitable and declaratory relief and attorneys' fees and costs.

127. Unless and until enjoined and restrained by order of this Court, the wrongful conduct of Defendant will continue to cause great and irreparable injury to Plaintiff and Class

members in that Defendant will continue to engage in the unlawful conduct alleged herein. Plaintiff and Class members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the unlawful conduct of Defendant.

COUNT THREE
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631
(On behalf of Plaintiff and the Class)

128. Plaintiff restates and realleges the allegations of paragraphs 1 through 96, above, as though fully set forth herein.

129. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

130. The California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, sets forth its purpose as follows:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

131. Under the CIPA, "any person who has been injured by a violation of [the CIPA] may bring an action against the person who committed the violation . . . ." Cal. Penal Code § 637.2(a).

132. A violation of § 631(a) of the CIPA occurs if, among other things, a person "by means of any machine instrument, or contrivance, or in any other manner":

> [i] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or

> [ii] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state, or
>
> [iii] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or
>
> [iv] aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above . . . .

Cal. Penal Code § 631(a) (paragraph numbers and line breaks added for readability).

133. The applicability of Cal. Penal Code § 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the internet, and email. *See Matera v. Google Inc*., 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (the CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc*., 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (the CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

134. In violation of the CIPA, Defendant aided, and agreed and conspired with the Third-Party Tracking Companies to permit and cause to be done proscribed conduct under § 631(a) of the CIPA, as alleged herein, including but not limited to integrating and embedding the Third-Party Tracking Companies' tracking technologies into the Website.

135. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA or constitute "any other manner" as used in the CIPA:

(a) The computer codes and programs of the Third-Party Tracking Companies used to intercept, monitor, capture and record Plaintiff's and Class members' communications while they were accessing and navigating the Website;

(b) Plaintiff's and Class members' browsers;

(c) Plaintiff's and Class members' computing and mobile devices;

(d) The web servers of the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members';

(e) The web servers from which the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members intercepted Plaintiff's and Class members' communications while they were using a web browser to access and navigate the Website;

(f) The computer codes and programs used by the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members to effectuate their interception and recording of Plaintiff's and Class members' communications while they were using a browser to access and navigate the Website;

(g) The plan the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Class members carried out to effectuate their interception of Plaintiff's and Class members' communications while they were using a web browser or mobile application to access and navigate the Website; and

(h) The code of the Third-Party Tracking Companies Defendant procured to

intercept the communications of Plaintiff and Class members embedded, integrated and installed into the Website.

136. Plaintiff and Class members did not consent to the unlawful conduct of Defendants PowerSchool and Heap, as alleged herein.

137. Among the contents of communications, data transmissions and messages the Third-Party Tracking Companies intercepted, read, attempted to read and learned were the contents of Plaintiff's and Class members' confidential education records and the information contained therein.

138. By engaging in the unlawful conduct alleged herein, Defendant violated Plaintiff's and Class members' statutorily-protected right to privacy.

139. On information and belief, Defendant's violations of the CIPA, as alleged herein, occurred in California.

140. As a result of the conduct alleged herein, under the CIPA, Defendant is liable to Plaintiff and each Class member in the amount of, the greater of, $5,000 dollars per violation or three times the amount of actual damages.

141. Unless and until enjoined and restrained by order of this Court, the wrongful conduct of Defendant will continue to cause great and irreparable injury to Plaintiff and Class members because Defendant will continue to unlawfully tap and intercept the contents of students' communications within the Website while they access and navigate the Website. Plaintiff and Class members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the unlawful conduct of Defendant.

COUNT FOUR
Violation of the Illinois Eavesdropping Act
720 Ill. Comp. Stat. 5/14-1, *et seq.*
(On behalf of Plaintiff and the Illinois Subclass)

142. Plaintiff restates and realleges the allegations of paragraphs 1 through 96, above, as though fully set forth herein.

143. Plaintiff brings this claim individually and on behalf of the members of the proposed Illinois Subclass against Defendant.

144. Under the Illinois Eavesdropping Act, 720 Ill. Comp. Stat. 5/14-1, *et seq.*, it is unlawful for a person to knowingly and intentionally "intercept[], record[], or transcribe[], in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication." 720 Ill. Comp. Stat. 5/14-2(a)(3).

145. Under the Illinois Eavesdropping Act, an injured party is entitled to civil remedies against both the eavesdropper and the eavesdropper's principal. 720 Ill. Comp. Stat. 5/14-6.

146. Under the Illinois Eavesdropping Act, a "private electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 Ill. Comp. Stat. 5/14-1(e).

147. Under the Illinois Eavesdropping Act, "surreptitious" means "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 Ill. Comp. Stat. 5/14-1(g).

148. Under the Illinois Eavesdropping Act, an "eavesdropper" is "any person, including any law enforcement officer and any party to a private conversation, who operates or participates

in the operation of any eavesdropping device contrary to the provisions of [the Illinois Eavesdropping Act] or who acts as a principal . . . .” 720 Ill. Comp. Stat. 5/14-1(b).

149. Under the Illinois Eavesdropping Act, an “eavesdropping device” is “any device capable of being used to hear or record oral conversations or intercept or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means.” 720 Ill. Comp. Stat. 5/14-1(a).

150. Under the Illinois Eavesdropping Act, a “principal” is any person who: “(1) [k]knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) [k]nowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) [d]irects another to use an eavesdropping device illegally on his or her behalf.” 720 Ill. Comp. Stat. 5/14-1(c).

151. Under the Illinois Eavesdropping Act, the information Plaintiff and Illinois Subclass Members sent and received while using the Website, including video purchasing information and education records, constituted – and continue to constitute – private electronic communications.

152. Under the Illinois Eavesdropping Act, the following constitute eavesdropping devices, as they are capable of being used to record and intercept electronic communications, including the electronic communications of Plaintiff and Illinois Subclass members while accessing and navigating the Naviance platform:

(a) The computer codes and programs of the Third-Party Tracking Companies used to intercept, monitor, capture and record Plaintiff’s and Illinois Subclass members’ communications and data transmissions while they were accessing and navigating the Website;

(b) Plaintiff's and Illinois Subclass members' browsers;

(c) Plaintiff's and Illinois Subclass members' computing and mobile devices;

(d) The web servers of the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Illinois Subclass members';

(e) The web servers from which the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Illinois Subclass members intercepted Plaintiff's and Illinois Subclass members' communications while they were using a web browser to access and navigate the Website;

(f) The computer codes and programs used by the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Illinois Subclass members to effectuate their interception and recording of Plaintiff's and Illinois Subclass members' communications while they were using a browser to access and navigate the Website;

(g) The plan the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Illinois Subclass members carried out to effectuate their interception of Plaintiff's and Illinois Subclass members' communications while they were using a web browser or mobile application to access and navigate the Website; and

(h) The code of the Third-Party Tracking Companies Defendant procured to intercept the communications of Plaintiff and Illinois Subclass members embedded, integrated and installed into the Website.

153. Defendant was, and continues to be, an eavesdropper under the Illinois Eavesdropping Act because it acted, and continues to act, as a principal. Defendant was, and continues to be, a principal under the Illinois Eavesdropping Act because it: (a) knowingly derives and derived a benefit and information from the illegal use of the eavesdropping devices of third parties, including the Third-Party Tracking Companies, whose tracking technologies Defendant integrated, installed and embedded into the Website – including detailed information about students who use and used the Website, including Plaintiff and Illinois Subclass members; and (b) directed third parties, including the Third-Party Tracking Companies, to illegally use an eavesdropping device on Defendant's behalf.

154. The unlawful conduct of Defendant, as alleged herein, has injured Plaintiff and Illinois Subclass members and entitles them to actual and punitive damages.

155. Unless and until enjoined and restrained by order of this Court, the wrongful conduct of Defendant will continue to cause great and irreparable injury to Plaintiff and Illinois Subclass members in that Defendant will continue to engage in the unlawful conduct alleged herein. Plaintiff and Illinois Subclass members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the unlawful conduct of Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff seeks a judgment against Defendant, individually and on behalf of all others similarly situated, as follows:

(a) Certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) Declaring that Defendant's conduct violates the statutes referenced herein;

(c) Finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) Awarding statutory damages to the extent available;

(e) Awarding prejudgment interest on all amounts awarded;

(f) Ordering injunctive relief as pleaded or as the Court may deem proper; and

(g) Awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b)(1), Plaintiff demands a trial by jury of all issues so triable.

Dated: April 1, 2025

Respectfully submitted,

Janielle Dawson, individually and on behalf all others similarly situated

By: /s/ Scott R. Drury
SCOTT R. DRURY
One of Plaintiff's attorneys

Scott R. Drury
DRURY LEGAL, LLC
6 Carriage Lane
Highwood, Illinois 60040
Telephone: (312) 358-8225
E-Mail: scott@drurylegal.com

Joshua D. Arisohn (to be admitted *pro hac vice*)
ARISOHN LLC
513 Eighth Avenue, #2
Brooklyn, NY 11215
Telephone: (646) 837-7150
Email: josh@arisohnllc.com

Attorneys for Plaintiff and putative class members